How and Why to Protect Operational Technology Systems

Antonio Mario Durante **(Head of Space & Defence Development Support Services, RINA Consulting S.p.A)**
Giorgio Gentile **(Manager - Software Engineering & Cyber-Security, RINA Consulting S.p.A)**

As cybersecurity breaches of industrial control systems (ICS) continue to increase, two things are clear. Firstly, information technology (IT) is converging with operational technology (OT) – hardware or software that monitors or controls physical devices and processes. Secondly, while most companies now take IT cybersecurity seriously, many underestimate security risks from the OT in their industrial control systems.

INTRODUCTION

Inadequate protection may cause significant financial loss, injury or environmental damage. However, ICS are often considered safe as they are "not connected to the internet" or "not based on vulnerable technologies". For this reason, they are not subject to regular updates or security assessments. For operational reasons, though, systems are occasionally connected to a company network or to a standalone PC. If these are not fully secure, opportunistic malware can easily penetrate the ICS and damage or block the system. A targeted attack, perhaps designed to steal data or blackmail a company, would be child's play.

There are four key elements:

1) OT cyber threats increasingly resemble those of IT systems: dynamic, constantly renewed and exploiting vulnerabilities in individual components;
2) Vulnerabilities may derive from interdependencies or operational changes. Initial checks and certifications do not ensure security during the system's entire life cycle;
3) Continuous system security management is essential and staff should be trained to maintain system security;
4) A series of measures must work in combination to increase the system's resilience and protect critical components.

These four elements point to one conclusion: we need to consider the system throughout its life. When advising on IT/OT security at RINA, we focus on developing a cost-effective approach that is tailored to our client's specific needs and covers the system's entire life cycle.

Some principles are:

1) Ensure that everyone involved in the system life cycle, including component manufacturers, integrators and end users, contributes to managing system security;
2) Extend security assessments beyond the initial system release phase;
3) Make the supplier responsible for continually assessing cyber risks to the system or components and informing the customer of new vulnerabilities;
4) Develop a robust cyber risk analysis process;
5) Conduct regular staff training and checks;
6) Regularly assess cyber risks for producers, integrators and users to verify the system's protection and resilience;
7) Implement a two-way process for recording incidents and sharing information between the contractor and the client.

RINA's services cover the whole engineering process, from the definition of the security requirements to the design, implementation and verification of measures to mitigate the identified risks. Following a "through-life" process and methodology, we ensure that the security of the system is achieved by design and maintained throughout the whole life cycle and contractual chain, from the designer to the operator and back again.

THE ISSUE

The Operational Technology (OT) systems / networks (as the ones used in Industrial Control Systems (ICS)) are composed by a collection of devices designed and connected together as a whole. A fail in a device may harm or jeopardise the whole network causing a domino effect with catastrophic consequences.

In past years there have been a few targeted attacks to Industrial Control Systems that became well known to the community. One of the most (in) famous successful attacks is the one linked to the STUXNET worm. This worm was specifically developed to target specific Programmable Logic Controllers (PLCs) exploiting zero-day vulnerabilities. In other words, targeting an Industrial Control System required specific and in-depth knowledge of the system, its behaviour and a means to introduce the "malicious code" within the system. Usually, the easiest way to gain access to an ICS is through an insider, be it - as an example, an operator or maintainer, doing it in an intentional or unintentional way.

In fact, until recently, OT systems were designed as closed systems disconnected from the world. This means that a factory or a ship management system were accessible only from a terminal deployed on-site. Moreover, OT systems were implemented using components which were ad-hoc designed and built.

OT systems often perform simple but essential tasks, such as monitoring a valve and shutting it off when a threshold value is triggered. As a result, they could face no changes or very little changes for years, as long as they perform their tasks. This means that these systems sometimes run on aging operating systems and obsolete hardware using home grown applications.

Since the goal for an OT system is to run exactly as designed, even patches are only applied if they do not hinder the process of the OT system. This approach was deemed as a secure and safe one, as the system was confined to the location of deployment and, hypothetically, disconnected from the rest of the world.

Over the course of the years, IT products have largely evolved. They got more and more multipurpose and cheaper. This aspect made IT components from being attractive to being one of the most used choices for the implementation of OT systems.

This convergence between IT and OT is however under estimated by many. It is a matter of facts that information and cyber security breaches in IT and Industrial Control Systems continue to increase, but while many recognizes the need to invest in cybersecurity in IT applications and face the continuously evolving threat scenario, few recognizes this risk and need for Industrial Control Systems.

This aspect together with the main differences between these two worlds, as it will be highlighted in the following, are such to encourage considering Industrial Control Systems/OT systems as critical, if not more, than IT systems from a cyber security point of view. While similar for many aspects they are very different from a conceptual point of view. The table below summarises the main differences between these two worlds.

Table 1: Differences between IT and OT

IT	OT
Focused on the information management	Focused on the operation/process
High dynamicity in changing/evolution	**Low dynamicty in changing/evolution.**
Many users and highly exposed.	**Few users and well trained.**
Dynamic threat and in continuous evolution.	Static threat sticking to the design phase.
Short life cycle.	**Long life cycle.**
Highly interconnected systems, by definition.	Traditionally isolated systems.
Limited or no attention at all to safety risks.	**High attention to safety risks.**
High attention to cyber risks.	No attention or very limited attention to cyber risks.
No safety critical systems.	**Evaluation and management of safety critical systems.**

Highlighted in bold are those elements that are today proper of the industrial control systems obtained by the convergence of the IT and OT world. The most strident conflict is the one between **long life cycle** and **dynamic threat in continuous evolution**. This means that Industrial Control Systems are meant to face a daily changing menace leveraging on a project designed to last years with no or little modification.

Adopting IT technology to implement ICSs and interconnecting them to the internet - directly or indirectly - to remotely monitor or control their behavior and status exposes these systems to the cyber threats proper of IT systems. This means that it is no more required a specific knowledge to develop a malware targeting and harming a control system but a generic IT malware could do the work in the same way.

This scenario, although looking not likely or very unlikely, already happened in 2017. The malware we're talking about was the largely known and recognized WANNACRY. This ransomware was developed to infect systems, encrypt its content and request ransom payments in exchange of the information. Moreover, it was built to replicate over the network the affected system was connected to.

WANNACRY was reported to have affected over 150 countries and more than 300'000 computers, among which there were some being part of an Industrial Control System. As an example, Toyota and Renault had stop two of their production lines following an infection by the ransomware.

In addition to untargeted attacks and multipurpose malware, cyber-attacks have risen to an unprecedented level of sophistication. What once was represented by simple experiments or isolate computer enthusiasts challenging themselves are now turning into sophisticated activities performed for profit or other socio-political reasons. There are

even companies and divisions within states/governments providing this kind of service.

Attackers have various motives, skills, and relationships, though these may often be ignored when focusing on security solutions to defeat their efforts. Gaining a better understanding of the motivational, social, political and economic forces at work in the hacking community provides substantive context to understand how social forces shape the nature of new emerging cyber threats.

This aspect is also relevant for critical infrastructures since they are controlled, monitored and operated by Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems that have becoming more accessible remotely via the Internet.

In this matter it is worth mentioning that it exists a search engine, named SHODAN, which crawls the internet for devices (e.g. IoT, ICS, etc) remotely connected and indexes them.

These search engines provide an anonymous reconnaissance platform that facilitates ICS targeting for those actors with both a desire and capability to carry out attacks.

This point is very important as it completely goes against one of the core principles against which most of the ICS were initially designed: the isolation from the outer world.

However, thinking to resolve the cybersecurity matter adopting technical countermeasures only is not feasible, at least in the OT world. ICS are meant to monitor a system and help an operator to make it working.

This sentence is true because of two main factors:

1) The implementation of technical measures on an industrial control system will not always solve the problem. On the opposite, they will create new points of attention. In fact, technical measures are meant to work on a - deliberately complicated - simple and repeatable logic. They cannot make reasoning behind a certain behaviour or system value. They will behave as programmed. This means that even a slight out of range parameter but still in the safe zone, if not properly modelled it could promptly bring to a stop of the system.
2) Industrial control systems are systems conceived to perform operations and carry on a process in a continuous way and with no halts. Operators are meant to control the systems and ensure they are behaving as designed and as expected.

Operators - and human beings in general- will always play an important part in the OT world.

In fact, they cannot be completely controlled by technical measures and they could be the enabling factor for vulnerabilities or unwanted/unexpected system behaviour, if not properly trained or made aware of the consequences.

One of the most underrated issues for ICSs, from a cyber security point of view is the one related to maintenance. Often, maintenance is outsourced. This means that maintainers are (or at least could be) not aware of the security rules and the importance security covers in our system.

This could lead to malicious behaviours, like for example, disabling a security rule to ease their work or connect a not secure/not trusted device to our network, jeopardising the whole system.

It may sound as a joke, but it happened that a whole system had to be shut down and recovered because a maintainer put in charge their smartphone, connecting it to the USB port of a server. The smartphone was carrying malicious code and was set to be mounted as an hard drive. As soon as it was plugged to, hypothetically, recharge, the malicious code affected the server and started replicating all over the network, infecting other systems and going forward.

The correct training of an operator is not just a matter of providing them with a class on how to use the system or what shall not be done.

The training and awareness topics are part of a bigger picture.

These aspects shall not be stand-alone topics but they shall be part and shall be derived from an information management system, where the requirements and the processes are described.

Not only the operator shall be aware of that but the whole company shall be aware of how the system operates and which are the security requirements and implications if they are not met.

However, humans are not the only potential vulnerability in ICSs.

At least they are not from an operational point of view only. In fact, the design and implementation of the system are as important as their operation and maintenance.

At design phase, an important point to be taken into account and to be tangled is the one deriving from interdependencies and interconnections among systems.

In fact, it doesn't matter how much we secure our system if the systems we are relying on or providing services to are not as hardened as ours.

This aspect, however, cannot always be completely foreseen and solved by the designer. However it can be addressed identifying

a set of security requirements to be reflected to the other providers or customers in terms of security level agreement within the service level agreement.

As for the training, achieving this objective is only possible with a proper management system in place at company level. The requirements shall be well known by all the stakeholders involved in the process: from the purchase office to the facility management and up, again, to the management.

Due to the fact that cyber security is under the loupe as a major threat, all working groups in different domains - like aviation, maritime, etc - are trying to find a way to give a regulatory body to this issue and try to solve it in a structured way.

One of the mostly debated aspects is the need or not for a cyber security certification to be applied to products.

The main problem behind this possibility is related to the high dynamicity of the threat evolution and the evolution of the technological counterpart.

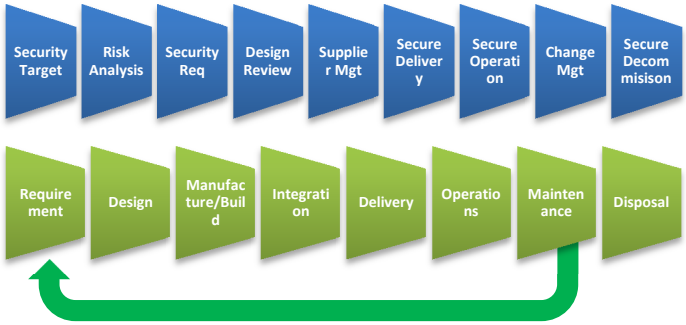
In fact, a product certified as “cyber approved” or “cyber resilient” today, it will not likely be applicable in a 3 months period. Therefore, shall a system be certified or re-evaluated every 3 months, the certification process shall be very fast and cheap.

The closest certification concerning cyber security applied to IT systems is the one related to Common Criteria, ISO15408. But this is the closest in terms of topic and not at all in terms of time and budget.

This is why, one of the solutions that is being investigated by RINA is the one to move the attention from the product itself and focus on the product lifecycle process.

RINA is willing to apply the security-by-design principle to cyber security worthiness evaluation.

Figure 1: Security by Design Illustration



The chosen approach allows building trust and confidence in the end-users that the company producing a system is well aware of the cyber menace and that has means and processes in place to face it and react to it, in case of need.

As an example, this means having detailed processes and procedures for the management of the security requirements at design phase and their verification during the development and testing phase. Or, again, this means having clear and auditable processes concerning the maintenance of the security requirements during the whole system lifecycle process, being clear which are the processes to follow to upgrade the system and how to ensure that there is no regression on all the functionalities.

As it can be seen on the chart above, the security affects all the steps of the lifecycle and shall be extended/reflected to the whole supply chain.

CONCLUSION

In fact, ensuring the security of the system is not a matter of the single but it’s a shared effort.

Being aware of this will drastically improve security and mutual trust while, hopefully, reducing costs deriving from incidents and system halts or recovery.